IA-00109

Information Assurance Vulnerability Alert DISA Internal Process and System

Jacqueline Price Snouffer
jackie.snouffer@ritchie.disa.mil
(7 17) 267-9997

9 February 1999

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 09021999	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Information Assurance Vulnerability Alert DISA Internal Process and System	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) DISA	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms "IATAC COLLECTION"	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 22	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
2/9/99

3. REPORT TYPE AND DATES COVERED
Briefing

4. TITLE AND SUBTITLE
Information Assurance Vulnerability Alert DISA Internal Process and System

5. FUNDING NUMBERS

6. AUTHOR(S)
Jacqueline Price Snouffer

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This briefing outlines DISA's internal procedure for tracking IAVAs. It discusses the policy, procedures, organizations responsible for tracking the IAVAs, and the security features of the program.

14. SUBJECT TERMS
DISA, vulnerability

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT
UNCLASSIFIED

20. LIMITATION OF ABSTRACT
None

IAVA Background

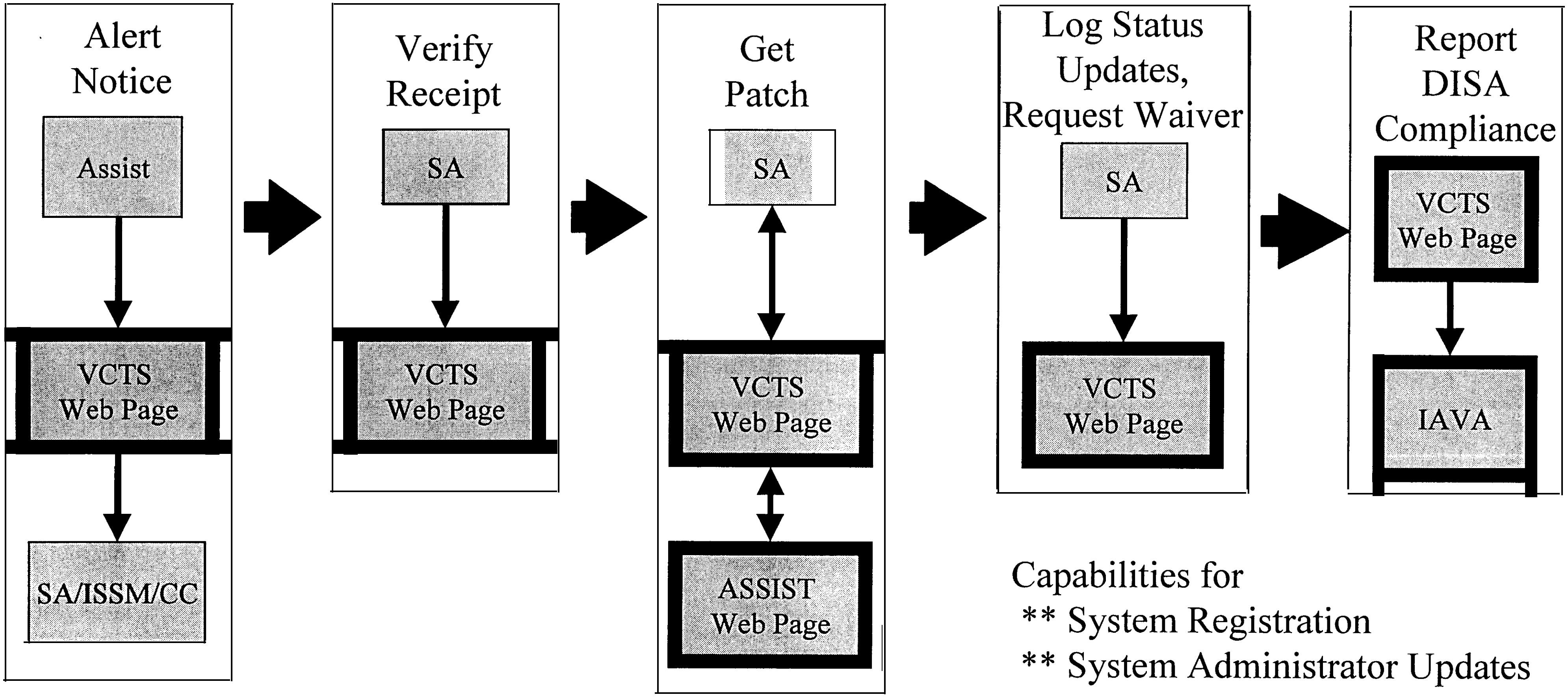
DOD has mandated that all C/S/A develop a methodology for ensuring:

- Vulnerability alert notifications are received by System Administrators
- Vulnerabilities are corrected within 30 days
- Periodic/Random validation of system status

Vulnerability Compliance Tracking System

- Provide the ability to quickly notify and receive acknowledgement from subordinates of an IAVA
- Assess the impact of a vulnerability on the infrastructure
- Monitor status and closure of vulnerabilities
- Provide reporting to DoD of compliance

Vulnerability Compliance Tracking System



Alert Notice

Assist

VCTS Web Page

SA/ISSM/CC

Verify Receipt

SA

VCTS Web Page

Get Patch

SA

VCTS Web Page

ASSIST Web Page

Log Status Updates, Request Waiver

SA

VCTS Web Page

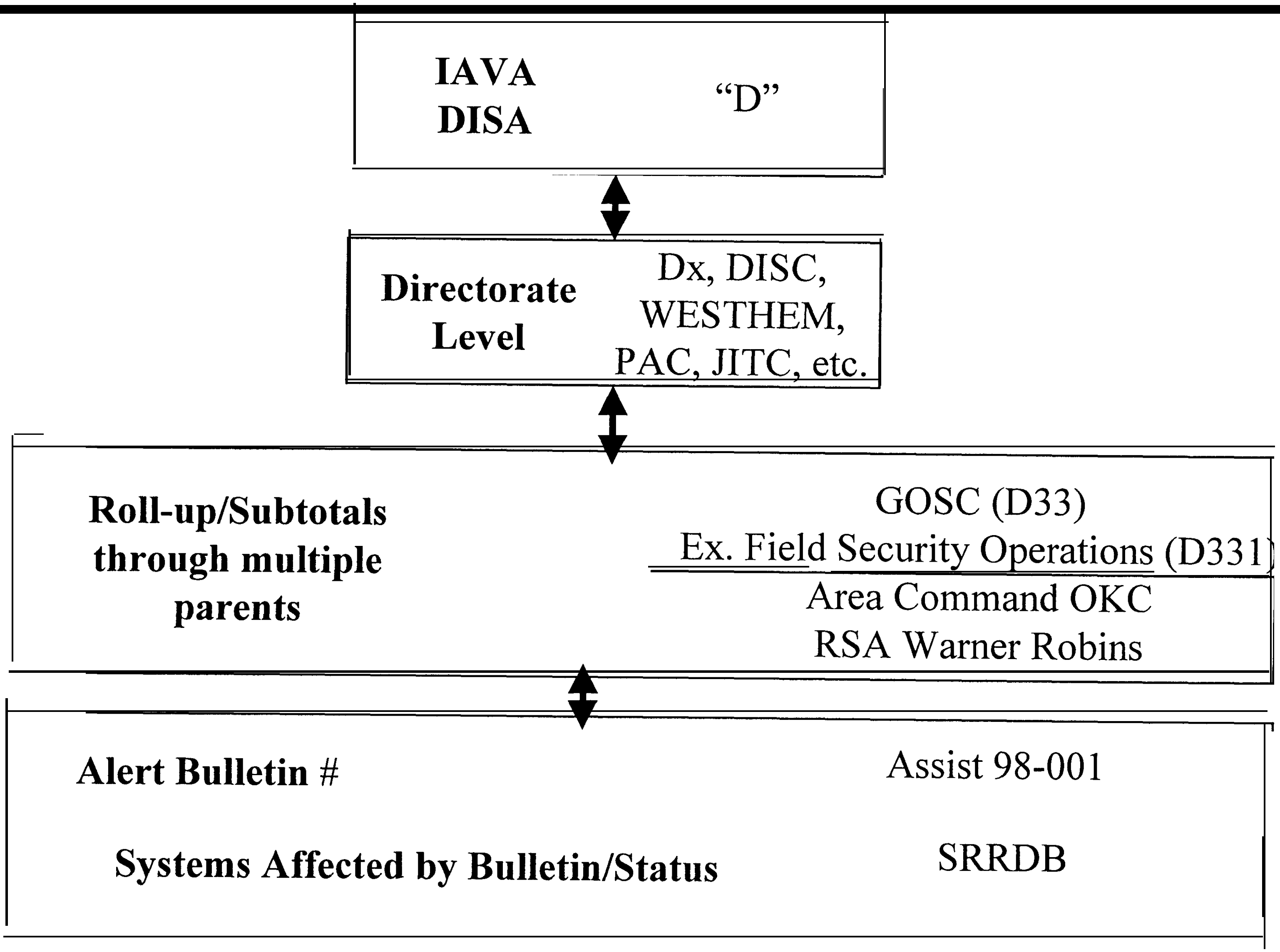
Report DISA Compliance

VCTS Web Page

IAVA

Capabilities for
** System Registration
** System Administrator Updates and Permissions

Organization Reporting Capability



IAVA
DISA

"D"

Directorate Level

Dx, DISC, WESTHEM, PAC, JITC, etc.

Roll-up/Subtotals through multiple parents

GOSC (D33)
Ex. Field Security Operations (D331)
Area Command OKC
RSA Warner Robins

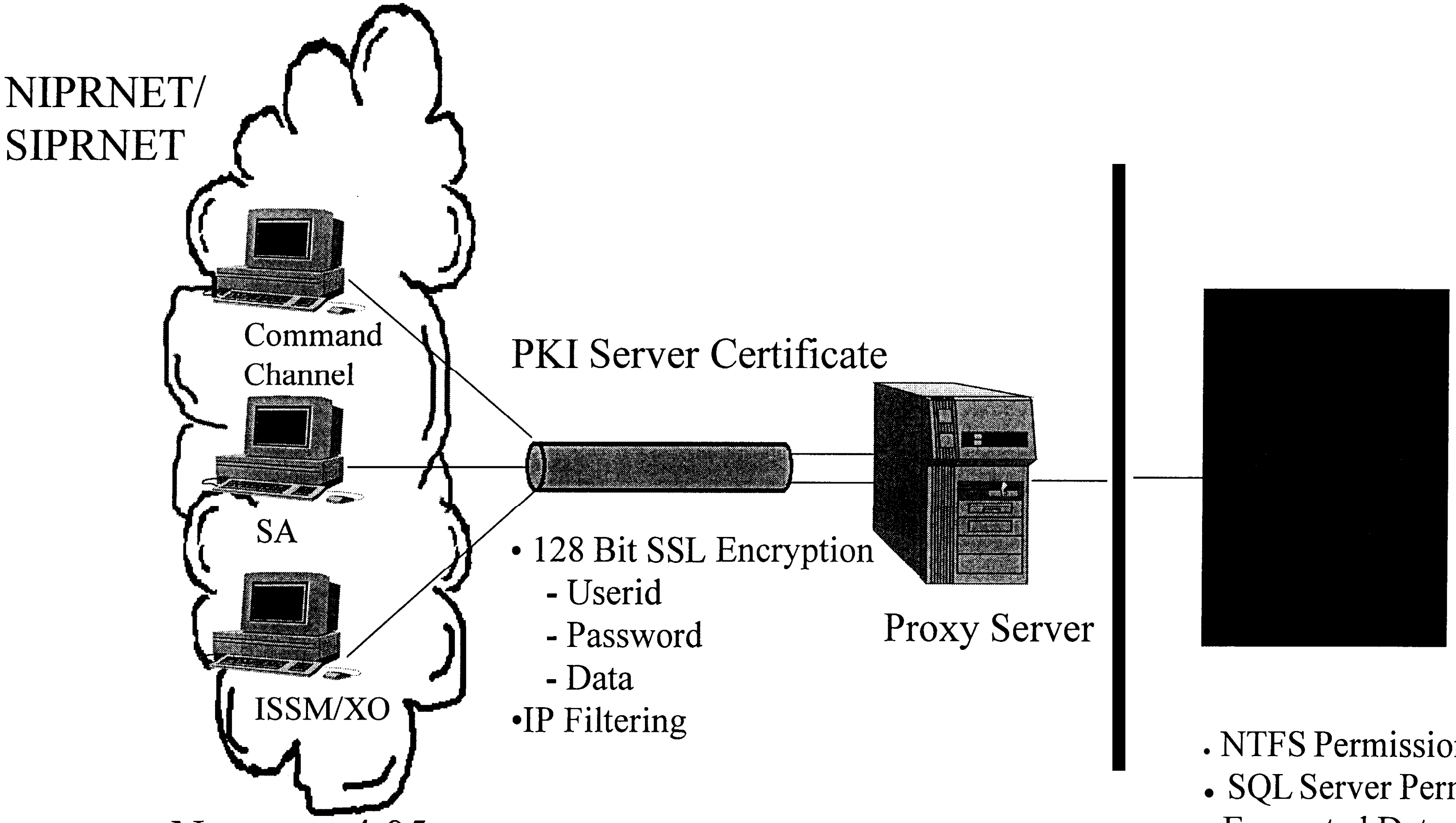
Alert Bulletin #

Assist 98-001

Systems Affected by Bulletin/Status

SRRDB

VCTS Security Features



[redacted]

- 128 Bit SSL Encryption
  - Userid
  - Password
  - Data
- IP Filtering

- NTFS Permissions
- SQL Server Permissions
- Encrypted Data
- Daily Backups
- Monitoring

- Netscape 4.05 or
- IE 4.0

Other Agency Use of VCTS

- Host on platform with DISA
  - Data segregated with strict access control
  - Costs to be negotiated

- POC
  - Danette Wile
  - 717-267-9933
  - wiled@ritchie.disa.mil

BACKGROUND

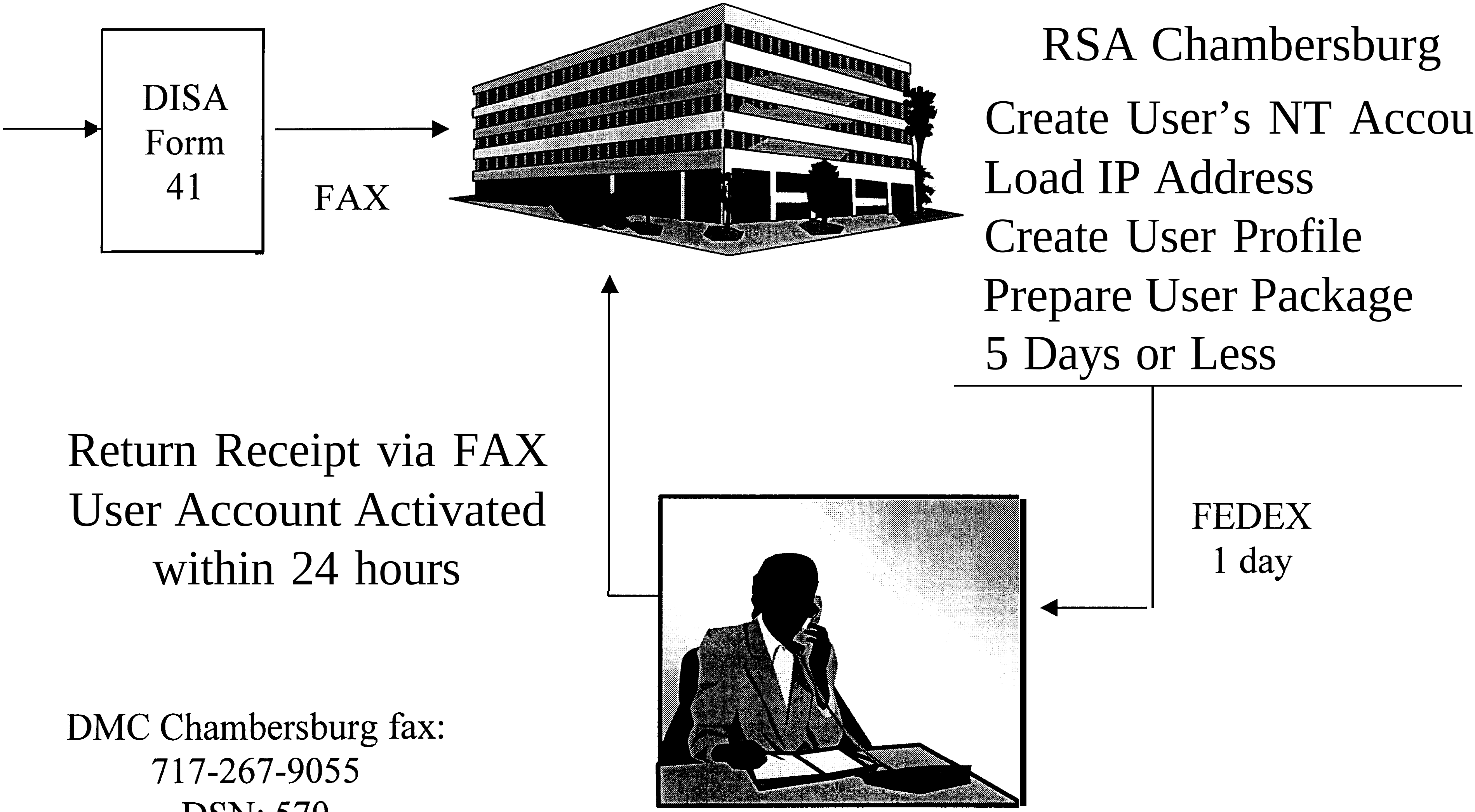
VCTS Capabilities

- Reporting/Oversight by ISSMs and Xos
- Update of SA/User information
- Registration/Update of Systems
- Delegation of browse & update to other SAs
- Automatic feed to IAVA of DISA's posture

Vulnerability Compliance Tracking System (VCTS) Capabilities

- Notification of alert to registered users based on function
- Acknowledgement of receipt by system
- Process for requesting waivers
- Tracking of closure/posture of vulnerabilities

VCTS Registration Process



DISA Form 41

FAX

RSA Chambersburg

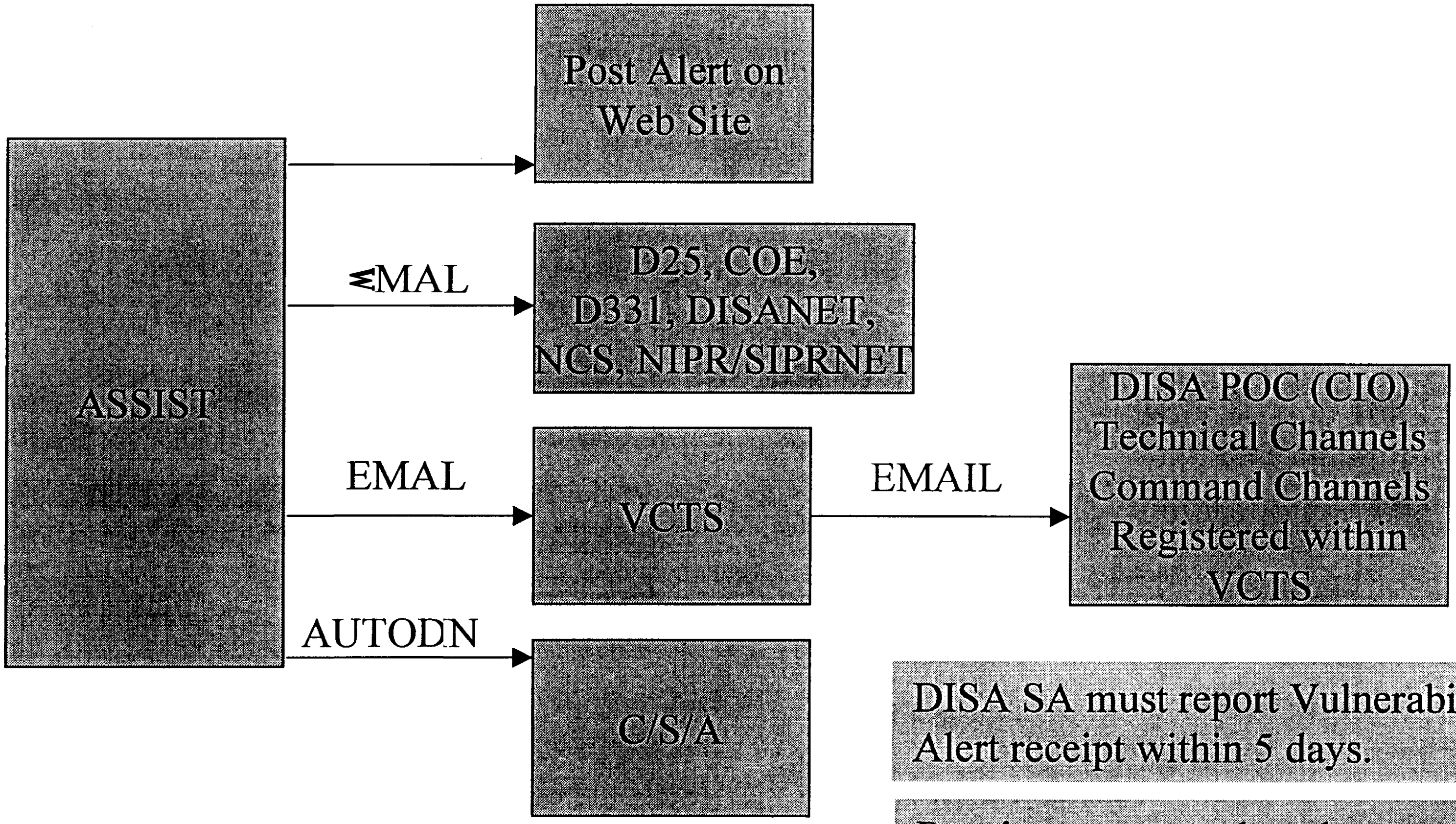
Create User's NT Account
Load IP Address
Create User Profile
Prepare User Package
5 Days or Less

FEDEX
1 day

Return Receipt via FAX
User Account Activated
within 24 hours

DMC Chambersburg fax:
717-267-9055
DSN: 570

Message Dissemination



ASSIST

Post Alert on Web Site

≤MAL

D25, COE, D331, DISANET, NCS, NIPR/SIPRNET

EMAL

VCTS

EMAIL

DISA POC (CIO) Technical Channels Command Channels Registered within VCTS

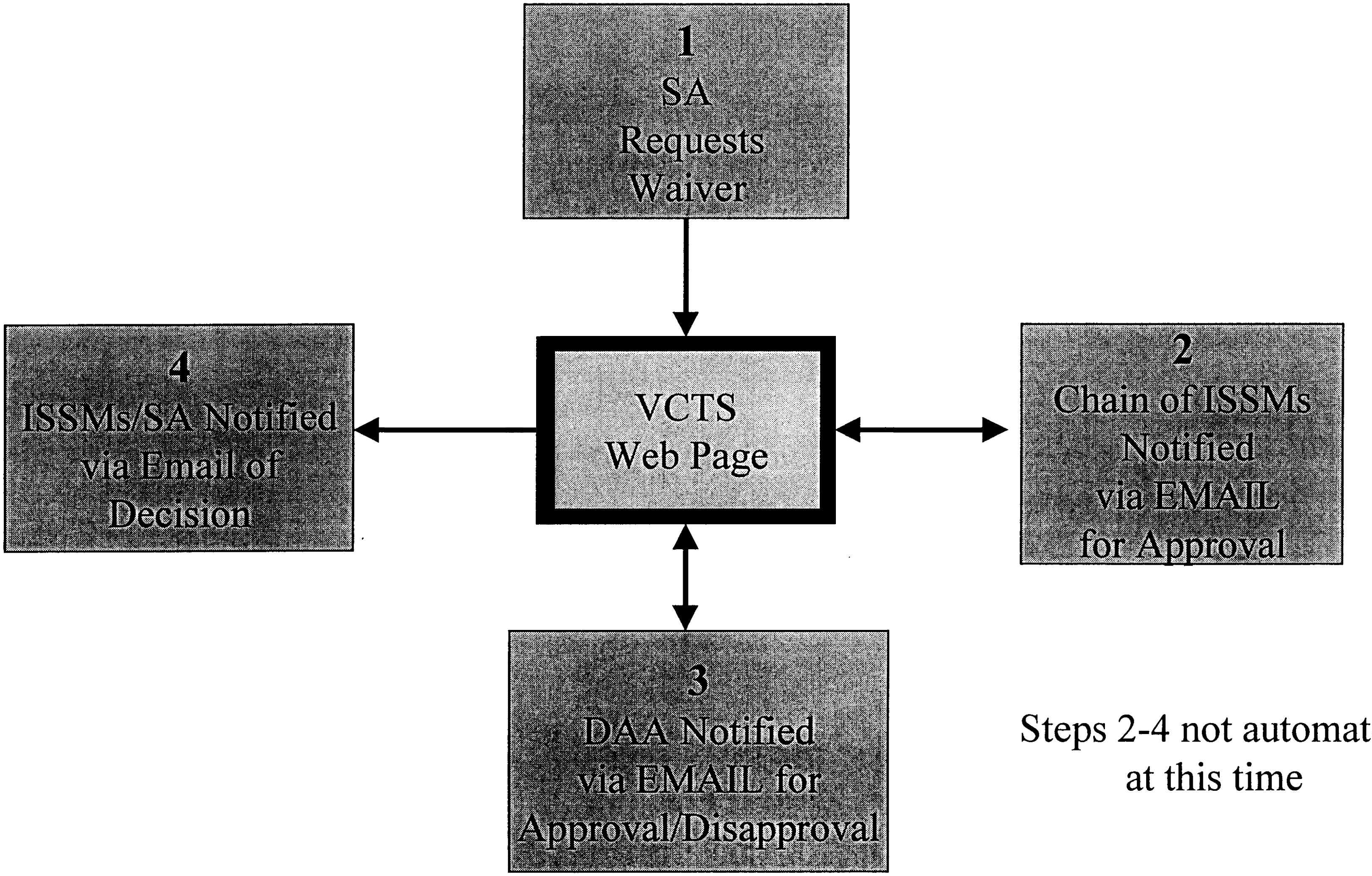
AUTODN

C/S/A

DISA SA must report Vulnerability Alert receipt within 5 days.

Receipt counts are kept by system so that only one SA from each system needs to report for all systems affected.

Walver Process



Steps 2-4 not automated
at this time

User Types

- XO
  - Receive all IAVA Alerts
  - Organizational view of the data
  - Notified when waiver has been requested

- ISSM
  - Receive all IAVA Alerts
  - Organizational view of the data
  - Approves waiver prior to DAA adjudication

User Types

- System/Network Administrators
  - Recieves only those bulletins for systems they have registered or have been given update authority for
  - Requests waiver
  - Cannot view system data that they have not been given explicit permission to

Current Reports Available

- ISSM/XO
  - – Compliance Summary Report by Vulnerability (VM02)
  - – Active Users by Organization (VM03)
  - – Registered Systems by Organization (VM04)
  - – Waiver Summary Spreadsheet (VM08)

- SA/ISSM/XO
  - – Compliance/Acknowledgement Report by System (VSO 1)
  - – Compliance/Acknowledgement Report by Vulnerability (VS02)

V 1.0 Outstanding Capabilities

- Complete Reporting
  - VS05/06 - Acknowledgement Report by User/System
    - By Organization/Site
    - By Alert
    - 1 March 1999
- Interim Waiver Process
  - CIO will grant/deny waivers regardless of accreditor
  - CIO will grant/deny waiver, indicate expiration date, and provide pertinent comments
  - Available 25 February 1999

V 2.0 Enhancements

- Link to Accredited System/Major Program
  - Allow for oversight by Program Management Office
  - Allow for Waiver Request/Granting for entire Program
  - Allow Email by PMO to SA(s)
  - Multiple accreditor based on system/program
  - Allow Accreditor to review site and system status
  - Allow Accreditor to review asset/component information
  - Cross Oganizational browsing at program level

V 2.0 Enhancements

- Fully automate waiver process
  - Through ISSM/Program/Technical/Adjudication Chain
  - Process for Major Programs to be determined by Program
  - Multiple DAAs
  - Ability to establish different waiver processes depending on program or system

- Specifications out for comment on 1 March 1999

V 2.x Requested Enhancements

- Status Information
  - Update status after completion
  - Allow browse by XO, ISSM, PMO, CIO
  - Provide list of N/A reasons
- Allow ISSM to enter Organizational Comment
- Acknowledgement
  - Unacknowledge Receipt
  - Confirm Acknowledgement

V 2.x Requested Enhancements

- Subscription to bulletins

- ISSM to give permission to a system within their organization to any registered SA

- Supporting reports for new functionality